



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,454	02/26/2004	Sarvar Patel	29250-002013/US	4912

7590 08/29/2008
HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 8910
Reston, VA 20195

EXAMINER

TOLENTINO, RODERICK

ART UNIT	PAPER NUMBER
----------	--------------

2134

MAIL DATE	DELIVERY MODE
-----------	---------------

08/29/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/786,454	Applicant(s) PATEL ET AL.	
	Examiner Roderick Tolentino	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 July 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1 – 24 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1 and 24 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rezaiifar et al. U.S. PG-Publication No. (2003/0206538) in view of Rose et al. U.S. PG-Publication No. (2004/0218763).
5. As per claims 1 and 24, Rezaiifar teaches the first cryptosync having a life limited to the communication session, based on a value of a second cryptosync, the second cryptosync having a life extending over multiple communication session (Rezaiifar, Paragraphs 0041 and 0042, cryptosyncs having time stamps and second cryptosyncs extending past the time stamp) but fails to teach deriving a value of a first cryptosync for the communication session. However, in an analogous art Rose teaches deriving a

value of a first cryptosync for the communication session (Rose, Paragraph 0056, key derived from previous key).

At the time the invention was made it would have been obvious, to a person of ordinary skill in the art to use Rose's system for replacing a cryptographic key with Rezaiifar's cryptosync for wireless communication system because it offers the advantage of having a convenient, efficient and confidential method for replacing keys (Rose, Paragraph 0008).

6. Claims 2 – 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rezaiifar et al. U.S. PG-Publication No. (2003/0206538) in view of Rose et al. U.S. PG-Publication No. (2004/0218763) in further view of Rezaiifar et al. U.S. Patent No. (6,980,658).

7. As per claim 2, Rezaiifar in combination with Rose fails to teach the second cryptosync is used for message encryption by at least one of the two devices. However, in an analogous art Rezaiifar teaches the second cryptosync is used for message encryption by at least one of the two devices (Rezaiifar, Col. 3 Lines 36 – 45, mobile devices and base stations).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art, to use Rezaiifar's method and apparatus for encrypting transmissions in a communication system with Rezaiifar's cryptosync for wireless communication system because it offers the advantage of maintaining encryption

protocols to prevent the disclosure of communications between parties (Rezaiifar, Col. 1 Lines 66 – 67 and Col. 2 Lines 1 – 2).

8. As per claim 3, Rezaiifar as modified teaches the second cryptosync is used for verifying message integrity by at least one of the two devices (Rezaiifar, Col. 2 Lines 39 – 48, verification).

9. As per claim 4, Rezaiifar as modified teaches the second cryptosync is used for verifying message integrity by at least one of the two devices (Rezaiifar, Col. 2 Lines 39 – 48, verification).

10. As per claim 5, Rezaiifar as modified teaches the second cryptosync changes between communication sessions (Rezaiifar, Col. 6 Lines 41 – 44, different cryptosyncs).

11. As per claim 6, Rezaiifar as modified teaches deriving step derives the first cryptosync as at least a portion of the second cryptosync (Rezaiifar, Col. 2 Lines 25 – 38, creates two cryptosync values).

12. As per claim 7, Rezaiifar as modified teaches the deriving step derives the first cryptosync as at least a portion of the second cryptosync and a fixed bit sequence (Rezaiifar, Col. 4 Lines 46 – 62, bit sequence).

13. As per claim 8, Rezaiifar as modified teaches the deriving step derives most significant bits of the first cryptosync as the portion of the second cryptosync and derives least significant bits of the first cryptosync as the fixed bit sequence (Rezaiifar, Col. 4 Lines 46 – 62, bit sequence).

14. As per claim 9, Rezaiifar as modified teaches the fixed bit sequence is a string of 0s (Rezaiifar, Col. 9 Lines 11 – 22, EID value of Zero).

15. As per claim 10, Rezaiifar as modified teaches the deriving step derives a 32 most significant bits of the first cryptosync as the second cryptosync and derives a 32 least significant bits of the first cryptosync as a string of 0s (Rezaiifar, Col. 9 Lines 11 – 22, EID value of Zero).

16. As per claim 11 Rezaiifar n as modified teaches the deriving step derives a portion of the first cryptosync as the second cryptosync (Rezaiifar, Col. 2 Lines 25 – 38, creates two cryptosync values).

17. As per claim 12, Rezaiifar as modified teaches the deriving step derives a first portion of the first cryptosync as the second cryptosync and derives a second portion of the first cryptosync as a fixed bit sequence (Rezaiifar, Col. 4 Lines 46 – 62, bit sequence).

18. As per claim 13, Rezaiifar as modified teaches the fixed bit sequence is a string of 0s (Rezaiifar, Col. 9 Lines 11 – 22, EID value of Zero).

19. As per claim 14, Rezaiifar as modified teaches the deriving step comprises: performing a pseudo-random function on the second cryptosync; and generating the first cryptosync from output of the pseudo-random function (Rezaiifar, Col. 8 Lines 15 – 21, randomly chosen).

20. As per claim 15, Rezaiifar as modified teaches the generating step generates the first cryptosync as the output of the pseudo-random function (Rezaiifar, Col. 8 Lines 15 – 21, randomly chosen).

21. As per claim 16, Rezaiifar as modified teaches the deriving step is performed at a base station (Rezaiifar, Col. 3 Lines 36 – 45, mobile devices and base stations).
22. As per claim 17, Rezaiifar as modified teaches the deriving step is performed at a mobile station (Rezaiifar, Col. 3 Lines 36 – 45, mobile devices and base stations).
23. As per claim 18, Rezaiifar as modified teaches encrypting a frame of information to send from the at least one of the two devices using the first cryptosync (Rezaiifar, Col. 2 Lines 19 – 23, encryption).
24. As per claim 19, Rezaiifar as modified teaches the frame of information is a radio link protocol, RLP, frame (Rezaiifar, Col. 6 Lines 45 – 56, RLP frames).
25. As per claim 20, Rezaiifar as modified teaches incrementing the first cryptosync after the encrypting step (Rezaiifar, Col. 2 Lines 38 - 48, incrementing).
26. As per claim 21, Rezaiifar as modified teaches decrypting a frame of information received at the at least one of the two devices using the first cryptosync (Rezaiifar, Col. 5 Lines 56 – 67, decryption).
27. As per claim 22, Rezaiifar as modified teaches the frame of information is a radio link protocol, RLP, frame (Rezaiifar, Col. 6 Lines 45 – 56, RLP frames).
28. As per claim 23, Rezaiifar as modified teaches incrementing the first cryptosync after the decrypting step (Rezaiifar, Col. 2 Lines 38 – 48, incrementing).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on Monday - Friday 9am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Roderick Tolentino
Examiner
Art Unit 2134

Roderick Tolentino
/R. T./
Examiner, Art Unit 2134

/ELLEN TRAN/
Primary Examiner, Art Unit 2134